

## Podstawowe informacje dotyczące Cyberbezpieczeństwa

### 1. Silne i Bezpieczne Hasła – Twoja Pierwsza Linia Obrony!

Hasło jest jak klucz do Twojego cyfrowego domu. Jeśli będzie słabe, ktoś łatwo może się tam włamać.

- **Twórz długie hasła** – dobre hasło powinno mieć co najmniej 12–14 znaków.
- **Mieszaj znaki** – używaj wielkich i małych liter, cyfr oraz znaków specjalnych (np. @, #, !, \*).
- **Zrezygnuj z oczywistości** – nie używaj swojego imienia, daty urodzenia ani prostych ciągów typu 123456.
- **Jedno hasło do jednego konta** – nigdy nie używaj tego samego hasła w różnych miejscach (np. do e-dziennika i do gry online).
- **Korzystaj z menedżera haseł** – to bezpieczny program, który zapamięta wszystkie trudne hasła za Ciebie.
- **Włącz dwuskładnikowe uwierzytelnianie (2FA)** – to dodatkowa ochrona, która przy logowaniu wymaga wpisania kodu wysłanego np. na Twój telefon. Włącz je wszędzie, gdzie to możliwe!

### 2. Phishing – Nie Daj się Złowić na Haczyk!

**Phishing** (czyt. fiszing) to metoda oszustwa. Przestępcy podszywają się pod znane firmy, kurierów, a nawet pod szkołę, aby ukraść Twoje hasła lub pieniądze.

- **Sprawdzaj adres nadawcy** – oszuści używają adresów, które na pierwszy rzut oka wyglądają znajomo, ale mają małe błędy (np. pomoc@alllegro.pl zamiast allegro.pl).
- **Uważaj na ponaglenia** – wiadomości typu „Zablokujemy Twoje konto w ciągu 24 godzin!” to niemal zawsze oszustwo. Presja czasu ma uśpić Twoją czujność.
- **Nie klikaj w podejrzane linki** – zawsze wpisuj adres strony ręcznie w przeglądarce, zamiast klikać w odnośniki z niepewnych wiadomości.
- **Zwracaj uwagę na błędy** – język pełen błędów ortograficznych lub dziwnych zwrotów to znak ostrzegawczy.

### 3. Bezpieczna Poczta Elektroniczna

Szkolna i prywatna skrzynka e-mail to miejsca, przez które przesyłamy wiele ważnych informacji.

- **Nie otwieraj nieznanych załączników** – pliki z rozszerzeniami .exe, .scr czy .zip od nieznajomych mogą zawierać wirusy, które uszkodzą Twój komputer.
- **Wyloguj się po skończonej pracy** – jeśli korzystasz z komputera w pracowni szkolnej lub bibliotece, zawsze pamiętaj o kliknięciu „Wyloguj”. Samo zamknięcie karty w przeglądarce nie wystarczy!
- **Ogranicz zaufanie** – pamiętaj, że nauczyciel, dyrektor ani pracownik banku nigdy nie poproszą Cię w e-mailu o podanie Twojego hasła.

## 4. Ochrona Urządzeń i Danych Osobowych

Twój smartfon, tablet i komputer potrzebują stałej ochrony przed złośliwym oprogramowaniem.

- **Aktualizuj system i aplikacje** – aktualizacje naprawiają luki bezpieczeństwa, dlatego instaluj je regularnie.
- **Używaj programu antywirusowego** – dobry program ochroni Twoje urządzenie przed wirusami.
- **Pobieraj pliki z legalnych źródeł** – gry i aplikacje ściągać tylko z oficjalnych sklepów (Google Play, App Store). „Darmowe” wersje płatnych gier bardzo często zawierają ukryte wirusy.
- **Chroń swoją prywatność** – nie udostępniaj w sieci swojego adresu zamieszkania, numeru PESEL, zdjęć dokumentów ani informacji, że cała rodzina wyjeżdża na wakacje.
- **Zabezpiecz ekran blokady** – telefon zawsze powinien być zablokowany kodem PIN, wzorem lub odciskiem palca.

## 5. Jak Reagować na Podejrzane Zdarzenia?

Co zrobić, gdy coś pójdzie nie tak? Najważniejsze to **nie panikować** i działać według planu:

1. **Odłącz urządzenie od sieci** – jeśli podejrzewasz, że pobrałeś wirusa lub ktoś się włamał, odłącz Wi-Fi lub kabel sieciowy. To odetnie oszusta od Twojego urządzenia.
2. **Zmień hasła** – jeśli przypadkowo wpisałeś hasło na podejrzanej stronie, natychmiast zaloguj się na prawdziwą stronę i zmień je na nowe.
3. **Poinformuj dorosłego lub specjalistę**
  - **Uczniu:** Powiedz rodzicom, wychowawcy lub szkolnemu pedagogowi.
  - **Nauczycielu / Pracowniku:** Zgłoś incydent szkolnemu administratorowi sieci lub dyrekcji.
4. **Zgłoś oszustwo odpowiednim służbom**
  - Podejrzane wiadomości SMS można bezpłatnie przekazać do zespołu **CERT Polska** na numer **2808**.
  - Podejrzane strony internetowe i e-maile zgłaszaj bezpośrednio poprzez oficjalny formularz na [incydent.cert.pl](http://incydent.cert.pl).

---

*Pamiętaj: Bezpieczeństwo w Internecie zależy przede wszystkim od naszych codziennych nawyków. Bądź uważny i dbaj o siebie w cyfrowym świecie!*

---